

AO 106 (Rev. 04/10) Application for a Search Warrant

AUTHORIZED AND APPROVED/DATE: s/Daniel Gridley, Jr. 8-21-24

## UNITED STATES DISTRICT COURT

for the  
Western District of Oklahoma

In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)TWO WIRELESS CELL PHONES CURRENTLY STORED IN  
THE CUSTODY OF USPIS LOCATED AT 6500 AIR CARGO  
RD OKLAHOMA CITY, OK 73195

Case No. M-24- 635 -SM

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

Located in the Western District of Oklahoma, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section  
 21 U.S.C. § 846  
 21 U.S.C. § 841(a)(1)

Offense Description  
 Drug Conspiracy  
 Possession of Controlled Substances with Intent to  
 Distribute

The application is based on these facts:

See attached Affidavit of Chris Nicholson, United States Postal Inspector

- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: (\_\_\_\_\_) ) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Chris Nicholson, United States Postal Inspector

Printed name and title

Sworn to before me and signed in my presence.

Date:

Aug. 22, 2024

City and state: Oklahoma City, Oklahoma



Judge's signature

Suzanne Mitchell, United States Magistrate Judge

Printed name and title

**IN THE UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF OKLAHOMA**

**IN THE MATTER OF THE  
SEARCH OF: TWO WIRELESS  
CELL PHONES CURRENTLY  
STORED IN THE CUSTODY OF  
USPIS LOCATED AT 6500 AIR  
CARGO RD OKLAHOMA CITY,  
OK 73195**

**M-24- 635-SM**

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Chris Nicholson, being duly sworn, do hereby depose and state:

## INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—two wireless cell phones of various make, model, and color that are currently stored in the custody of the United States Postal Inspection Service (USPIS) located at 6500 Air Cargo Road, Oklahoma City, Oklahoma 73195—and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Postal Inspector with USPIS and have been so employed since December 2021. I am currently assigned to the USPIS Fort Worth Division domiciled in Oklahoma City, Oklahoma. I am responsible for conducting investigations of crimes against the United States Postal Service in violation of federal law(s). My duties include

the investigation of illegal mailings and the receipt of controlled substances, possession of which violates Title 21, United States Code, Sections 841(a)(1) and 846.

3. Prior to becoming an Inspector for USPIS, I gained investigative experience as a Special Agent with the Naval Criminal Investigative Service (NCIS) from September 2017 to December 2021. My NCIS duties included, but were not limited to, investigating crimes committed against United States Navy assets and personnel worldwide, including allegations of espionage, fraud, theft, sexual assault, aggravated assault, child exploitation, and illegal drugs. My investigative experience has also been supplemented with numerous hours of participation with local and state law enforcement task forces to stay apprised of evolving criminal methodology.

4. Prior to NCIS, I was employed by the Dallas Police Department (DPD) from March 2007 to July 2013 as a Police Officer certified by the Texas Commission on Law Enforcement Standards and Education Basic Training Academy. During my time with DPD, I held investigative positions within burglary, narcotics, organized crime, and fugitive recovery squads. My employment with DPD required yearly in-service training, which included refresher courses in surveillance, warrant execution, tactics, criminal intelligence, and interview techniques. From 2013 to 2017, I was also employed as a Police Officer with the City of Kenner, Louisiana where I continued to perform the aforementioned duties.

5. Since becoming a federal agent, I have completed the Criminal Investigator Training Program and NCIS Special Agent Basic Training Academy at the Federal Law

Enforcement Training Center (FLETC), in Brunswick, Georgia, which included instruction in the investigation of federal, state, and local crimes.

6. While employed in a law enforcement capacity, I have made arrests for the aforementioned criminal activities and participated in the execution of approximately 100 search and seizure warrants authorized by federal and state judges. Throughout the last 17 years of my law enforcement career, I have conducted and assisted in numerous activities, to include, but not limited to, investigations, interviews, arrests, and the execution of search and seizure warrants, for crimes to include illegal drugs.

**IDENTIFICATION OF THE DEVICES TO BE EXAMINED**

7. The property to be searched includes two wireless cell phones of various make, model, and color (herein referred to as the “**TARGET DEVICES**”) as further described in **Attachment A** (physical description), for evidence of violations of 21 U.S.C. § 846, Drug Conspiracy, and 21 U.S.C. § 841, Possession with Intent to Distribute Controlled Substances as described further in **Attachment B** (description of items to be seized). The **TARGET DEVICES** are:

- i. A purple, Motorola cell phone, with black case and cracked screen, assigned USPIS PEAP# IS0001939280
- ii. A black Samsung cell phone assigned USPIS PEAP# IS0001939281

Both of the **TARGET DEVICES** are locked preventing investigators from obtaining additional specific identifying phone information such as a model or serial number. The **TARGET DEVICES** are currently stored in the custody of the

USPIS at 6500 Air Cargo Road, Oklahoma City, Oklahoma 73195 (Western District of Oklahoma).

8. The applied-for warrant would authorize the forensic examination of the **TARGET DEVICES** for the purpose of identifying electronically stored data particularly described in Attachment B.

9. This affidavit is based upon my personal investigation and information received by me from other law enforcement officers and agents. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

#### **PROBABLE CAUSE**

10. On August 9, 2024, while conducting a review of mail in transit to the USPS Processing and Distribution Center in Oklahoma City Oklahoma, USPIS located Priority Mail parcel 9505 5152 6931 4222 7845 81. Upon further investigation, this parcel displayed indicators consistent with the shipment of controlled substances, including the information contained in the subsequent paragraphs.

11. The parcel displayed hand-written sender and receiver information and was mailed from a zip code in Los Angeles, California (90044). The parcel was packaged in a white USPS Priority Mail (large) parcel with red and blue lettering. The parcel also had clear packing tape on the seams and weighted weighed approximately 11 pounds, 3.6 ounces. USPS records also indicated the parcel was paid for in cash in the amount of \$24.75.

12. Your affiant conducted postal computer database address verifications on the parcel and the database indicated the return address of “123 W 84<sup>th</sup> St LA, CA 90003”, as listed on the parcel, is a valid address. Utilizing CLEAR, a law enforcement accessible database which searches public and proprietary records, the sender’s name, “Angie Smith”, was not able to be associated with the return address.

13. Your affiant also checked databases for records of the delivery address on the parcel which indicated “321 SE 42<sup>nd</sup> St Oklahoma City, OK 73129”, as listed on the parcel, is a valid address. Utilizing the CLEAR database, the receiver's name, “Kendall Miles”, was able to be associated with the delivery address.

14. On August 10, 2024, your affiant conducted a background check on Kendall Miles revealing his status as a convicted felon. Miles’ criminal record indicated charges for possession of a controlled dangerous substance (hallucinogen), possession of a controlled dangerous substance (cocaine), and possession of a controlled dangerous substance with intent to distribute.

15. Gregory Griffin was also associated with the recipient address via computer database checks. Griffin is also a convicted felon with prior charges of possession of a controlled dangerous substance-PCP, possession of a controlled dangerous substance and possession of proceeds derived from a violation of the Uniform Controlled Substance Act.

16. On August 11, 2024, your affiant removed the parcel from the mail-stream and transported it to the USPIS Oklahoma City Domicile where it was secured for further investigation.

17. As background, since approximately April of 2024, USPIS has conducted surveillance on the on the recipient address due to this parcel's consistency with a series of delivered parcels displaying the same suspicious indicators. During prior surveillance, a black GMC pickup, driven by an older black male, was seen circling the recipient address before and after delivery. Registration checks on the vehicle revealed ownership by Gregory Griffin at 321 SE 42<sup>nd</sup> St Oklahoma City, OK. The vehicle would perform behavior consistent with counter-surveillance activity by parking at neighboring businesses and making several laps around the delivery address before ultimately parking and taking the parcel inside the residence.

18. On August 12, 2024, your affiant obtained and executed a search warrant for the aforementioned parcel revealing approximately 4,078 grams of liquid phencyclidine, commonly known as PCP. The PCP was logged as evidence in the USPIS Oklahoma City Domicile and planning began for a controlled delivery to the recipient address.

19. On August 13, 2024, your affiant participated in a controlled delivery of USPS Parcel 9505 5152 6931 4222 7845 81 to the recipient address of 321 SE 42<sup>nd</sup> St Oklahoma City, OK 73129. Due to the dangers of handling liquid PCP, and the concern for preserving evidence, the PCP was replaced with "sham" material which was placed inside the parcel. The parcel was then re-sealed for use in the controlled delivery.

20. On August 13, 2024, your affiant delivered the parcel to the front steps of 321 SE 42<sup>nd</sup> St Oklahoma City, OK. A short time later, the black GMC pickup truck arrived



in the driveway of the delivery address and a black male, later identified as Gregory Griffin, exited the vehicle. Griffin placed the parcel inside the residence and later returned to his truck without it. As Griffin was driving away from the residence, he was detained by law enforcement. At the same time, an anticipatory search warrant was executed at the residence. Upon law enforcement entry, an individual was detained who was later identified as Lamont Johnson with an active, but non-extraditable, arrest warrant out of California for trafficking illegal drugs. During his interview, Johnson advised his cell phone was inside the delivery address and provided a description of his phone which was consistent with **TARGET DEVICE 1**. Lying next to **TARGET DEVICE 1** was also **TARGET DEVICE 2**. During the search of the residence, numerous items of evidence were recovered in addition to the **TARGET DEVICES** to include suspected PCP, suspected MDMA, suspected cocaine base, a stolen handgun.

#### **BACKGROUND REGARDING CELLULAR DEVICES**

21. Based upon my training and experience, I am aware that individuals involved in fraudulent activity often use cellular phones to maintain contact with co-conspirators and purchasers of information illegally obtained from the U.S. Mail. Such cell phones and their associated memory cards commonly contain electronically stored information which constitutes evidence, fruits, and instrumentalities of fraud offenses including, but not limited to, the phone directory and/or contacts list, calendar, text messages, voicemail, e-mail messages, call logs, photographs, and videos. Additional items commonly found on cell phones are applications or “apps” that are self-contained programs designed to enhance functionality. Some of these apps include those such as Apple Wallet or Walgreens which



are used to purchase items in lieu of cash or a debit card. Both Apple Wallet and the Walgreens app require an account, created by the user, which includes personal and financial information. Once the account is completed, the app, combined with the cell phone, can be used for a convenient transaction experience.

22. Based upon my training and experience, I am aware that individuals involved in fraudulent activity often drop or switch phones to avoid detection by law enforcement, and often have multiple phones that they use for different co-conspirators in order to distance themselves from criminal activity. I am further aware that individuals involved in fraudulent activity often keep old cellular telephones no longer in use to save telephone numbers of co-conspirators, as well as other relevant information including text messages and photographs.

23. Based upon my training and experience, I am aware that individuals involved in illegal activity oftentimes have stored videos and/or text and voice messages maintained on their cell phones, which are associated with the use of fraudulently obtained mail and the proceeds derived from its use for furthering criminal activity.

24. Based upon my training and experience, I am aware that individuals involved in illegal activity often use coded words and phrases, as well as extremely vague conversations, in order to discuss their plans and prevent anyone from overhearing or recognizing that the subject matter involves illegal activity.

25. Based upon my training and experience, I am aware that individuals involved in illegal activity often use cellular telephones to perform payments for various items via the use of commercial financial applications such as Apple Wallet, Apple Pay, Google Pay,

Cash App, and Venmo. These financial applications require stored credit cards and/or bank account numbers, which, when involved in fraud, are commonly created from information illegally obtained from the US Mail system.

### **TECHNICAL TERMS**

26. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

### **ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

27. Based on my knowledge, training, and experience I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

28. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the **TARGET DEVICES** were used, the purpose of such use, who used the devices, and when. There is probable cause to believe that this forensic electronic evidence might be on the **TARGET DEVICES** because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

29. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device

consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

30. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

**AUTHORIZATION REQUESTS**

31. Based on the above information, there is probable cause to believe that violations of 21 U.S.C. § 846, Drug Conspiracy, and 21 U.S.C. § 841, Possession with Intent to Distribute Controlled Substances have occurred, and that evidence, fruits, and instrumentalities of these offenses are located on the **TARGET DEVICES**. Therefore, I respectfully request that this Court issue a search warrant for the **TARGET DEVICES**, described in **Attachment A**, authorizing the seizure of the items described in **Attachment B**.

  
CHRIS NICHOLSON  
Inspector  
United States Postal Inspection Service

Sworn and subscribed to before me this 22<sup>nd</sup> day of August 2024.

  
SUZANNE MITCHELL  
United States Magistrate Judge  
Western District of Oklahoma



**ATTACHMENT "A"**

**TARGET DEVICE 1:** A purple, Motorola cell phone, with black case and cracked screen, assigned USPIS PEAP# IS0001939280. **TARGET DEVICE 1** is locked, preventing investigators from obtaining additional specific identifying phone information. **TARGET DEVICE 1** is currently located in the custody of the United States Postal Inspection Service at 6500 Air Cargo Road, Oklahoma City, Oklahoma 73195 (Western District of Oklahoma).





**TARGET DEVICE 2:** A black Samsung cell phone assigned USPIS PEAP# IS0001939281. **TARGET DEVICE 2** is locked, preventing investigators from obtaining additional specific identifying phone information. **TARGET DEVICE 2** is currently located in the custody of the United States Postal Inspection Service at 6500 Air Cargo Road, Oklahoma City, Oklahoma 73195 (Western District of Oklahoma)



**ATTACHMENT "B"**

All records on **TARGET DEVICE 1 and 2 (TARGET DEVICES)** described in Attachment A that relate to violations of law, including 21 U.S.C. § 846, Drug Conspiracy, and 21 U.S.C. § 841, Possession with Intent to Distribute Controlled Substances, involving Lamont Johnson and possible co-conspirators. These records include:

- a. Stored communications to include voice recordings/messages, text messages (SMS) and multimedia messages (MMS), emails and attachments, read or unread, which relate to and provide evidence of criminal activity described in this affidavit;
- b. Stored communications voice or text based located within downloadable messaging applications or social media applications;
- c. All internet usage history that may reveal evidence of illegal drugs, such as package tracking, internet mail communications, electronic payment receipts, etc.;
- d. Call logs/histories depicting incoming/outgoing numbers dialed to and from the **TARGET DEVICES**;
- e. Internet World Wide Web (WWW) browser files including browser history, browser cache, browser favorites, auto-complete form history and stored passwords;
- f. Contacts, address books, calendars, customer lists and related identifying

information such as names, nicknames and/or monikers within the **TARGET DEVICES** which relate to and provide evidence of illegal drugs;

- g. Photographs, audio, and video recordings with their associated metadata;
- h. Stored location information including global positioning system (GPS) data indicating coordinates, way points, tracks and locations in which the **TARGET DEVICES** have traveled; and,

Evidence of user attribution showing who used or owned the **TARGET DEVICES** at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

**MANNER OF SEARCH AS TO VIDEOS, PHOTOGRAPHS, AND STORED COMMUNICATIONS**

Based upon my training and experience, I know that relevant and/or incriminating text or voice messages, videos, and photographs oftentimes are comingled on cellular telephones and electronic handheld devices with text messages, videos, and photographs which do not have an evidentiary value. However, criminals engaged in communications furthering the nature of their criminal enterprise often use cryptic, guarded, or otherwise coded jargon, which is often utilized to conceal the nature of their illegal communication. As a result, a limited review of the content of each communication will be necessary to determine the nature of the communication and whether it is relevant to that information particularly set forth above within this affidavit.

Searching the **TARGET DEVICES** for the evidence described above may require a range of data analysis techniques. In some cases, it is possible for agents to conduct



carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. For example, agents may be able to execute a keyword search that searches through the files stored in an electronic device for special words that are likely to appear only in the materials covered by a warrant. Similarly, agents may be able to locate the materials covered in the warrant by looking for particular directories or file names. In other cases, however, such techniques may not yield the evidence described in the warrant. Criminals can mislabel or hide files to evade detection, or take other steps designed to hinder law enforcement searches for information. These steps may require agents to conduct more extensive searches, such as scanning areas of the device's memory not allocated to listed files or opening every file and scanning its contents briefly to determine whether it falls within the scope of the warrant. In light of these difficulties, I request permission to use whatever data analysis techniques necessary to locate and retrieve the evidence described above.